

CLAIMS

We claim:

5 1. A method of authenticating concealed and statistically varying multi-dimensional data, the method comprising the steps of:

acquiring an initial measurement of an item, wherein the initial measurement is subject to measurement error;

10 applying a transformation to the initial measurement to generate reference template data;

acquiring a subsequent measurement of the item, wherein the subsequent measurement is subject to measurement error;

applying the transformation to the subsequent measurement; and

15 calculating a Euclidean distance metric between the transformed measurements; wherein the calculated Euclidean distance metric is identical to a Euclidean distance metric between the measurements prior to transformation.

2. The method of claim 1 wherein the steps of applying the transformation generate data that is substantially indistinguishable from Gaussian white noise.

3. The method of claim 1 wherein the steps of applying the transformation comprise
20 normalizing the measurements.

4. The method of claim 3 wherein the normalizing step comprises centering and scale-transforming the measurements so that mean and standard deviation are fixed.

5. The method of claim 1 wherein the steps of applying the transformation comprise permuting the measurements.

25 6. The method of claim 5 wherein permuting comprises employing an item of secret information.

7. The method of claim 6 wherein permuting comprises employing a passcode.

8. The method of claim 7 wherein permuting additionally comprises employing the results of a hash function of the passcode.

9. The method of claim 1 wherein the steps of applying the transformation comprise employing a linear transformation.

10. The method of claim 9 wherein employing a linear transformation comprises employing a transformation matrix with orthonormal columns.

5 11. The method of claim 10 wherein employing a linear transformation comprises employing a normalized Hadamard matrix.

12. The method of claim 10 wherein employing a linear transformation comprises employing a normalized matrix comprising Fourier coefficients with a cosine / sine basis.

10 13. The method of claim 9 wherein the employing a linear transformation comprises permuting the linearly transformed data.

14. The method of claim 13 wherein permuting the linearly transformed data comprises employing an item of secret information.

15 15. The method of claim 14 wherein permuting the linearly transformed data comprises employing a passcode.

16. The method of claim 15 wherein permuting the linearly transformed data additionally comprises employing the results of a hash function of the passcode.

17. The method of claim 1 wherein the measurements comprise biometric data.

20 18. The method of claim 17 wherein the measurements comprise measurements selected from the group consisting of fingerprints, retinal scans, facial scans, hand geometry, spectral data, and voice data.

19. The method of claim 17 additionally comprising the step of storing the reference template data on a smart card to be carried by an individual from whom the biometric data was taken.

25 20. The method of claim 1 wherein the measurements comprise spectral data.

21. The method of claim 20 wherein the measurements comprise weapons spectra.

22. The method of claim 1 additionally comprising the step of adding pseudo-dimensions to the measurements to enhance concealment.

23. A method of concealing multidimensional digital input data and maintaining an ability to authenticate the concealed data, the method comprising the steps of:

normalizing the input data;

permuting elements of the normalized data;

5 linearly transforming the normalized and permuted data with a transformation matrix; and

permuting the linearly transformed data to create the concealed data;

wherein the concealed data can be authenticated without conversion back into the input data.

10 24. The method of claim 23 wherein the normalizing step comprises centering and scale-transforming the data so that mean and standard deviation are fixed.

25. The method of claim 23 wherein permuting the linearly transformed data comprises employing an item of secret information.

15 26. The method of claim 23 wherein permuting elements comprises employing a passcode.

27. The method of claim 26 wherein permuting elements comprises employing the results of a hash function of the passcode.

28. The method of claim 23 wherein linearly transforming comprises employing a transformation matrix with orthonormal columns.

20 29. The method of claim 23 wherein permuting the linearly transformed data comprises employing an item of secret information.

30. The method of claim 29 wherein permuting the linearly transformed data comprises employing a passcode.

25 31. The method of claim 30 wherein permuting the linearly transformed data additionally comprises employing the results of a hash function of the passcode.

32. The method of claim 23 wherein the concealed data is substantially indistinguishable from Gaussian white noise.

33. The method of claim 23 wherein in the linearly transforming step the transformation matrix comprises a normalized Hadamard matrix.

34. The method of claim 23 wherein in the linearly transforming step the transformation matrix comprises a normalized matrix comprising Fourier coefficients with a cosine / sine basis.

35. The method of claim 23 wherein the input data comprises biometric data.

5 36. The method of claim 35 wherein the input data comprises data selected from the group consisting of fingerprints, retinal scans, facial scans, hand geometry, spectral data, and voice data.

37. The method of claim 35 additionally comprising the step of authenticating the transformed input data with reference template data stored on a smart card to be
10 carried by an individual from whom the biometric data was taken.

38. The method of claim 23 wherein the input data comprises spectral data.

39. The method of claim 38 wherein the input data comprises weapons spectra.

40. The method of claim 23 additionally comprising the step of adding pseudo-dimensions to the input data to enhance concealment.

15 41. A method of concealing and authenticating statistically varying multi-dimensional data, the method comprising the steps of:

acquiring a measurement of an item, wherein the measurement is subject to measurement error;

applying a transformation to the measurement to substantially conceal the measurement; and

20 authenticating the transformed measurement without removing concealment of the transformed measurement and without employing an error-correction algorithm.